UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/496,065	02/01/2000	N. Asokan	SZ998-041	5668

7590 07/27/2005

Anne Vachon Dougherty Esq
IBM Corp
3173 Cedar Rd
Yorktown Heights, NY 10598

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 07/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/496,065	ASOKAN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-26 and 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-26 and 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *07122005*.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 5/13/2005 was received and considered.

2. Claims 9-26 & 30 are pending.

3. Anne Dougherty (914-962-5910) was contacted on 7/12/2005 regarding the merits of the case. The detailed explanation appears in the Interview summary accompanying this Office Action.

Response to Arguments

4. Applicant's arguments with respect to claims 9-26 & 30 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments regarding prior art that is currently relied upon will be addressed below.

5. Applicant's response (p. 9) requested clarification on the status of claim 30. As applicant previously stated, claim 30 contains subject matter similar to claims 9 and 12 and therefore is rejected under similar rationale.

6. Applicant's response (p. 11, ¶1) argues that none of the prior art teaches communicating the terminal authentication directly. Applicant is reminded that the term "directly" is not in the claims. Further, it is suggested that none of the prior art teaches dynamically creating a user-specific authenticity output message. It is noted that this also is not in the claim language.

7. Applicant's response (p. 12, ¶1) suggests that Merritt does not disclose an authenticity output message. However, Merritt discloses a PSP, which is returned from the server to the user. Further, it is suggested that the Merritt server does not authenticate itself to the terminal. However, Merritt explicitly discloses mutual authentication between the terminal and the

server/host (Fig. 3). Further, it is suggested that the server does not generate an authenticity output message regarding the authenticity of the terminal. However, the Merritt server sends a PSP to the user after the terminal and server have engaged in mutual authentication (Fig. 3).

8. Applicant's response (p. 13) suggests that Merritt does not have means for conducting communications along a first trusted connection and a second trusted connection. Merritt discloses a single connection. However, when modified by Manduley, a second trusted connection is established between the server and the user device.

9. Applicant's response (p. 14) suggests that the prior art fails to teach an authentication component for verifying the authenticity of a terminal. However, as previously explained, the server engages in mutual authentication with the terminal (Fig. 3), each performing cryptographic operations which verify the other's authenticity (see also col. 5, lines 1-16).

10. Applicant's response (p. 15) suggests that Merritt lacks a message generation component because the message is read from a database and that the Examiner is incorrect in analogizing retrieving and displaying the PSP to the dynamic generation and display of the authenticity output message. However, Merritt discloses that the PSP is retrieved in response to the account information and sent to the user. The message is therefore generated, otherwise it could not be communicated. Any data read from a computer and sent to another constitutes generation of a message, such as is required for transmission over a communication line.

11. Applicant's response (p. 16) argues that Merritt does not teach or suggest that an authenticity message is delivered to the user, at all. However, as described above, a PSP is retrieved, upon mutual authentication of the server and terminal, and delivered to the user.

12. Applicant's response (pp. 11-21) argues that two separate connections are not shown in the art. The manner in which these connections are designated as separate is not provided in the specification. Applicant further argues various terms such as ("two distinct connections" and sending the authenticity output message "directly" to an element). It is noted that neither of these phrases are described or enabled in the specification and neither are recited in the claim language.

13. Applicant's response (p. 21, ¶2) argues that Lessin teaches away from the claimed invention. However, Lessin suggests entering the PIN into the device, which is trusted and therefore would not teach away. Furthermore, Lessin does not teach away from the combination of Merritt, Manduley and Hoss for the same reason.

14. Applicant's response (p. 21, ¶3) suggests that Daggar neither teaches nor suggests how Daggar would establish the authenticity of the card. This argument is persuasive. However, Manduley teaches that a smart card should be periodically authenticated by the issuing authority/server (col. 3, line 64 – col. 4, line 21) to allow the issuing authority/server to maintain control over issued cards (col. 1, lines 30-54).

Claim Rejections - 35 USC § 112

15. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

16. Claims 9-26 & 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not disclose the first trusted connection being separate from the second trusted connection and that the message is not delivered over the first trusted connection between the terminal and the server.

17. Claims 9-26 & 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not enable one of ordinary skill to "separate" the two connections and does not disclose how data is sent over one trusted connection without sending the data over the other.

18. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

19. Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear how the terminal will display the message if the message is explicitly not send to the terminal.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 9-18, 21-22, 25-26 & 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,475,756 to **Merritt** in view of U.S. Patent 5,737,423 to **Manduley** and U.S. Patent 5,412,192 to **Hoss**.

Regarding claims 9, 11-12, 14, 17, 21, 30, Merritt discloses a server/host (Fig. 1, #2), a communications component/communication line (col. 2, lines 48-64) for establishing and conducting communications along a first trusted connection with the terminal (Fig. 1, #9) and along a second trusted connection with said user input device (data transfers from the user's card to the host through the ATM) (Fig. 1, #9, col. 4, lines 46-51 & col. 6, lines 21-22) wherein the first trusted connection is separate from the second trusted connection (each have unique source/destination), receiver means for receiving at least one authentication request from said terminal (Fig. 3, #310 & #360), at least one authentication component for verifying the authenticity of the terminal (Fig. 1, #4, #8, Fig. 3, #315 & col. 4, line 58 – col. 5, line 17) and a message generation component for generating at least one authenticity output message/PSP (col. 4, lines 11-20) for delivery (from host to ATM screen) (Fig. 1, #3) and a storage location (Fig. 1, element 3) for storing a user-specific authenticity output message/PSP (col. 4, lines 11-20). Merritt lacks sending the authenticity output message to the device (user's card) over the second connection. However, Manduley teaches that smart cards are useful in secure transactions, particularly as an electronic purse (col. 1, lines 11-29) and that exchanging messages between a user and a smart card is useful to make sure the correct user is using the smart card (col. 2, lines 7-23 & col. 1, lines 41-56). More specifically, Manduley teaches that the smartcard contains an

LCD display that will, at the request of the server/issuing authority, display a message to the user (col. 3, lines 11-16, lines 47-58). This message can be a message requesting the user to enter a response (col. 3, lines 47-58) to authenticate the user's presence (col. 4, lines 7-15). The response is encrypted, thereby authenticating the card (col. 2, lines 7-15 & col. 4, lines 7-13). In this situation, the smart card is acting as a second interface to the server (rather than just the terminal). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt to send the authenticity output message to a smart card (second trusted connection). One of ordinary skill in the art would have been motivated to perform such a modification because smart cards are used in secure transactions to ensure the legitimate user of the card will be reading the messages and allow the user to respond, as taught by Manduley (col. 2, lines 7-23 & col. 1, lines 41-56). Merritt, as modified, lacks explicitly not sending the message along the first trusted connection between the terminal and the server. However, Hoss teaches that to allow a remote source to control a smart card at any time (col. 1, lines 29-32, col. 2, lines 1-7 & lines 1-59), the card contains an RF receiver that can display messages to the user (Fig. 1 & col. 3, lines 11-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt to send the authenticity message/PSP to the smart card over an RF link. One of ordinary skill in the art would have been motivated to perform such a modification to maintain access to the card anywhere, as taught by Hoss (col. 1, lines 29-32 & lines 54-66).

Regarding claim 10, Merritt discloses the host and the terminal negotiating a session key (col. 6, lines 54-62).

Regarding claim 13, Merritt discloses communicating a message to a user (Fig. 5, element 515).

Regarding claim 15, as best understood, Merritt discloses a terminal displaying a message (col. 3, lines 40-45).

Regarding claim 16, Merritt discloses accessing a database/lookup table that stores user-specific messages/PSPs (col. 7, lines 1-10).

Regarding claim 18, Merritt discloses authentication information contained on the card (col. 3, lines 64-67 and col. 4, lines 1-11) to be read by the terminal/ATM (Fig. 3). Merritt discloses a terminal displaying an authenticity output message/PSP in response to authentication (Fig. 5 and col. 3, lines 20-48).

Regarding claim 22, Merritt discloses a message/PSP taking many forms, such as a still image, a sequence of images, a video or an audio clip (col. 4, lines 16-23).

Regarding claim 25, Merritt discloses a smart card system, as described above, but lacks authenticating the card to the server. However, Manduley teaches that a smart card should be periodically authenticated by the issuing authority/server (col. 3, line 64 – col. 4, line 21) to allow the issuing authority/server to maintain control over issued cards (col. 1, lines 30-54). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate the user device to the server. One of ordinary skill in the art would have been motivated to perform such a modification to maintain control over issued cards, as taught by Manduley (col. 1, lines 30-54).

Regarding claim 26, Merritt discloses authenticating a user (Fig. 3, element 390).

22. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Merritt** in view of **Manduley** and **Hoss**, as applied to claim 12 above, in further view of U.S. Patent 4,799,061 to Abraham et al. (**Abraham**). Merritt, as modified, lacks the device authenticating itself to the terminal. However, Abraham teaches that components in a communication system should be authenticated prior to communicating any useful information (col. 1, lines 62-66 & col. 2, lines 4-16), specifically between a smart card and a terminal (Fig. 1) to protect against usage of an unauthorized terminal (col. 1, line 66 – col. 2, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt to require the smart card authenticate itself to the terminal. One of ordinary skill in the art would have been motivated to perform such a modification to protect against usage of an unauthorized terminal, as taught by Abraham (col. 1, line 62 – col. 2, line 16).

23. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Merritt** in view of **Manduley** and **Hoss**, as applied to claim 12 above, in further view of U.S. Patent 4,868,376 to Lessin et al. (**Lessin**). Merritt discloses a smart card system, as described above, but lacks the card requesting the user authenticate himself. Lessin teaches that by requiring the user enter a PIN, a card can prevent unauthorized access to data (col. 4, lines 7-11 and col. 8, lines 27-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Merritt's smart card system to request the user authenticate himself to prevent unauthorized access. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized access to data on the card, as taught by Lessin.

24. Claims 23 & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Merritt** in view of **Manduley** and **Hoss**, as applied to claim 21 above, in further view of **Schneier**. Merritt, as modified above, lacks partially outputting a message. However, Schneier teaches that SKEY is a known authentication protocol (as the PSP is used to authenticate the server/host). In SKEY, each entity has a list of numbers (message). One of the numbers is outputted to be recognized by the other entity (partial message) (page 53). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the SKEY protocol for authentication using a message/PSP. One of ordinary skill in the art would have been motivated to perform such a modification because an eavesdropper gains no information about the message in that each output of the message is used only once (page 53).

Conclusion

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703) 872-9306 - *(571) 273-8300 after July 15, 2005*
(for formal communications intended for entry)

Or:

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
July 11, 2005

David Y. Jung
Primary Examiner